CLAIMS

What is claimed is:

1. A gaming apparatus operatively connectable through a communication network to a gaming system server, the gaming apparatus comprising:

a gaming terminal, operable to execute game software;

a secure communication apparatus, communicatively coupled to the gaming terminal, and operable to provide network access control for gaming information exchanged between the gaming terminal and a communication network;

an access control apparatus, communicatively coupled to the gaming terminal, and operable to prevent unauthorized access to gaming information within the gaming terminal; and

an integrity apparatus, communicatively coupled to the gaming terminal, and operable to ensure integrity of the gaming information within the gaming terminal.

2. The gaming apparatus of claim 1, wherein the secure communication apparatus is operable to exchange gaming information that is selected from a group of information types that includes the game software, game configuration data, game play data, game performance data, server-determined game outcomes, gaming device operations software, maintenance information, security data, player data, marketing data, operations data, accounting data, electronic fund transfer data, and wagering account transfer data.

3. The gaming apparatus of claim 1, further comprising:

at least one user interface selected from a group of user interfaces that includes a control panel, buttons, a coin acceptor, a note acceptor, one or more electro-mechanical reels, a keypad, one or more speakers, a card reader, a card reader display, and a video display.

4. A gaming apparatus operatively connectable through a communication network to a gaming system server, the gaming apparatus comprising:

a gaming terminal, operable to execute game software; and

a secure communication apparatus, communicatively coupled to the gaming terminal, and operable to provide network access control for gaming information exchanged between the gaming terminal and the communication network.

5. The gaming apparatus of claim 4, wherein the secure communication apparatus is operable to exchange gaming information that is selected from a group of information types that includes the game software, game configuration data, game play data, game performance data, server-determined game outcomes, gaming device operations software, maintenance information, security data, player data, marketing data, operations data, accounting data, electronic fund transfer data, and wagering account transfer data.

6. The gaming apparatus of claim 4, wherein the secure communication apparatus is further operable to execute virtual private network application software.

7. The gaming apparatus of claim 4, wherein the secure communication apparatus is further operable to implement a virtual private network tunneling protocol.

8. The gaming apparatus of claim 4, wherein the secure communication apparatus includes one or more firewalls.

9. The gaming apparatus of claim 4, wherein the secure communication apparatus is further operable to execute a cryptographic method to ensure integrity of the gaming information.

10. A gaming apparatus operatively connectable through a communication network to a gaming system server, the gaming terminal comprising:

a gaming terminal, operable to execute game software; and

an access control apparatus, operable to prevent unauthorized access to gaming information within the gaming terminal.

11. The gaming apparatus of claim 10, wherein the access control apparatus is operable to prevent unauthorized access to the gaming information, which is selected from a group of

information types that includes the game software, game configuration data, game play data, game performance data, server-determined game outcomes, gaming device operations software, maintenance information, security data, player data, marketing data, operations data, accounting data, electronic fund transfer data, and wagering account transfer data.

12. The gaming apparatus of claim 10, further comprising:

a secure communication apparatus, communicatively coupled to the gaming terminal, and operable to provide network access control for gaming information exchanged between the gaming terminal and the communication network.

13. The gaming apparatus of claim 10, further comprising:

an integrity apparatus, operable to ensure integrity of the gaming information within the gaming terminal.

14. A gaming apparatus operatively connectable through a communication network to a gaming system server, the gaming terminal comprising:

a gaming terminal, operable to execute game software; and

an integrity apparatus, operable to ensure integrity of the gaming information within the gaming terminal.

15. The gaming apparatus of claim 14, wherein the integrity apparatus is operable to ensure integrity of the gaming information, which is selected from a group of information types that includes the game software, game configuration data, game play data, game performance data, server-determined game outcomes, gaming device operations software, maintenance information, security data, player data, marketing data, operations data, accounting data, electronic fund transfer data, and wagering account transfer data.

16. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to implement an authentication protocol to prevent unauthorized access to an encryption key.

17. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to prevent malicious software from accessing the gaming information within the gaming terminal.

18. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to detect intrusive network packets received by the gaming terminal.

19. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to monitor gaming information for deviations from one or more expected baselines.

20. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to detect vulnerabilities in the gaming terminal.

21. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to alter operations of the gaming terminal in response to detection of corrupt data.

22. The gaming apparatus of claim 14, wherein the first integrity apparatus is further operable to alter operations of the gaming terminal in response to detection of a failure of the gaming terminal.

23. The gaming apparatus of claim 14, further comprising:

a first secure communication apparatus, communicatively coupled to the gaming terminal, and operable to provide network access control for the gaming information exchanged between the gaming terminal and the communication network.

24. A gaming system server apparatus, operatively connectable through a communication network to one or more gaming terminals, the gaming system server apparatus comprising:

a gaming server;

a secure communication apparatus, communicatively coupled to the gaming server, and operable to provide network access control for gaming information exchanged between the gaming server and the communication network;

an access control apparatus, communicatively coupled to the gaming server, and operable to prevent unauthorized direct access to gaming information within the gaming server; and

an integrity apparatus, communicatively coupled to the gaming server, and operable to ensure integrity of the gaming information within the gaming server.

25. The gaming system server apparatus of claim 24, wherein the secure communication apparatus is operable to exchange gaming information that is selected from a group of information types that includes the game software, game configuration data, game play data, game performance data, server-determined game outcomes, gaming device operations software, maintenance information, security data, player data, marketing data, operations data, accounting data, electronic fund transfer data, and wagering account transfer data.

26. The gaming system server apparatus of claim 24, further comprising:

at least one user interface selected from a group of user interfaces that includes a keyboard, a graphical interface unit display, a monitor, a printer, a modem, a tape drive, a digital video disk drive, and a compact disk drive.

27. A gaming system comprising:

at least one first gaming apparatus, which includes

a gaming terminal, operable to execute game software,

a first secure communication apparatus, communicatively coupled to the gaming terminal, and operable to provide network access control for first gaming information exchanged between the gaming terminal and a communication network,

a first access control apparatus, communicatively coupled to the gaming terminal, and operable to prevent unauthorized access to gaming information within the gaming terminal, and

a first integrity apparatus, communicatively coupled to the gaming terminal, and operable to ensure integrity of the gaming information within the gaming terminal; and

at least one second gaming apparatus, operatively connectable through the communication network to the at least one first gaming apparatus, wherein the at least one second gaming apparatus includes

a gaming server,

a second secure communication apparatus, communicatively coupled to the gaming server, and operable to provide network access control for gaming information exchanged between the gaming server and the communication network,

a second access control apparatus, communicatively coupled to the gaming server, and operable to prevent unauthorized direct access to gaming information within the gaming server, and

a second integrity apparatus, communicatively coupled to the gaming server, and operable to ensure integrity of the gaming information within the gaming server.

28. The gaming system of claim 27, wherein the gaming information is selected from a group of information types that includes the game software, game configuration data, game play data, game performance data, server-determined game outcomes, gaming device operations software, maintenance information, security data, player data, marketing data, operations data, accounting data, electronic fund transfer data, and wagering account transfer data.

29. A gaming system comprising:

one or more secure gaming terminals, wherein selected ones of the one or more secure gaming terminals include a first secure communication apparatus, a first access control apparatus, and a first integrity apparatus; and

one or more secure gaming servers, wherein selected ones of the one or more secure gaming servers include a second secure communication apparatus, a second access control apparatus, and a second integrity control apparatus, and wherein the one or more secure gaming terminals and the one or more secure gaming servers are operatively connected through a communication network.

30. The gaming system of claim 29, wherein the communication network includes a dedicated private network.

31. The gaming system of claim 29, wherein the communication network includes a public network.

32. The gaming system of claim 29, wherein each of the first secure communication apparatus and the second secure communication apparatus includes at least one secure communication element.

33. The gaming system of claim 32, wherein the at least one secure communication element is selected from a group that includes a virtual private network application software, a virtual private network tunneling protocol software, a firewall, and a cryptographic protocol.

34. The gaming system of claim 33, wherein the cryptographic protocol is selected from a group that includes a message authentication code protocol, a one-way hash protocol, a public-key cryptography protocol, a digital signature protocol, a symmetric encryption protocol, and a random number generator protocol.

35. The gaming system of claim 33, wherein the firewall includes a programmable network processor.

36. The gaming system of claim 33, wherein the firewall includes an adaptive computing integrated circuit.

37. The gaming system of claim 29, wherein each of the first access control apparatus and the second access control apparatus include at least one access control element.

38. The gaming system of claim 37, wherein the at least one access control element is selected from a group that includes a person authentication protocol, a software authentication protocol, a person authorization protocol, and an administration method.

39. The gaming system of claim 38, wherein the person authentication protocol is selected from a group that includes a username authentication protocol, a password authentication protocol, a biometric authentication protocol, and an access token authentication protocol.

40. The gaming system of claim 38, wherein the person authorization protocol is selected from a group that includes a username authentication protocol, a password authentication protocol, a biometric authentication protocol, and an access token authentication protocol.

41. The gaming system of claim 38, wherein the software authentication protocol is selected from a group that includes a message authentication code protocol, a one-way hash protocol, a public-key cryptography protocol, a digital signature protocol, a symmetric encryption protocol, and a random number generator protocol.

42. The gaming system of claim 29, wherein each of the first integrity apparatus and the second integrity apparatus include at least one integrity element.

43. The gaming system of claim 42, wherein the at least one integrity element is selected from a group that includes an antivirus software, an antivirus scanner, an intrusion detection system, a data integrity system, an incident response protocol, a security management protocol, a vulnerability assessment protocol, and an authentication protocol.

44. A method comprising:

encrypting an executable software program to form a first encrypted executable software program;

receiving, at a first firewall, a plurality of first data packets that includes the first encrypted executable software program;

transmitting the plurality of first data packets when network layer information of the plurality of first data packets is verified against an access control list of the first firewall;

receiving, at a programmable network processor, the plurality of first data packets, wherein the programmable network processor is configured to inspect application layer information of the plurality of first data packets;

transmitting the plurality of first data packets when the application layer information of the plurality of first data packets is recognized as valid by the programmable network processor;

receiving, at a gaming system server, the plurality of first data packets;

decrypting the first encrypted executable software program received at the gaming system server to form a first decrypted version of the executable software program;

authenticating the first decrypted version of the executable software program using a first predetermined criteria;

encrypting the first decrypted version of the executable software program to form a second encrypted executable software program when the first decrypted version of the executable software program is determined to be authentic;

transmitting a plurality of second data packets that includes the second encrypted executable software program across a communication network;

receiving, at a gaming system terminal, the plurality of second data packets;

decrypting the second encrypted executable software program received at the gaming system terminal to form a second decrypted version of the executable software program;

authenticating the second decrypted version of the executable software program using a second predetermined criteria; and

enabling execution of the second decrypted version of the executable software program when the second decrypted version of the executable software program is determined to be authentic.

45. A method comprising:

encrypting, at a gaming system server, a first version of an executable software program to form a first encrypted executable software program; and

transmitting, across a communication network to a gaming system terminal, a plurality of data packets that includes the first encrypted executable software program.

46. The method of claim 45, further comprising:

authenticating the first version of the executable software program using a first predetermined criteria, prior to transmitting the plurality of data packets.

47. The method of claim 45, further comprising:

receiving, at the gaming system server, a plurality of data packets that includes a first encrypted executable software program; and

decrypting the first encrypted executable software program received at the gaming system server to form the first version of the executable software program.

48. A method comprising:

receiving, at a gaming system terminal, a plurality of data packets that includes an encrypted executable software program;

decrypting the encrypted executable software program to form a decrypted version of an executable software program;

authenticating the decrypted version of the executable software program using a predetermined criteria; and

enabling execution of the decrypted version of the executable software program when the decrypted version of the executable software program is determined to be authentic.

49. A computer-readable medium having program instructions stored thereon to perform a method, which when executed within an electronic device, result in:

encrypting, at a gaming system server, a first version of an executable software program to form a first encrypted executable software program; and

transmitting, across a communication network to a gaming system terminal, a plurality of data packets that includes the first encrypted executable software program.

50. A computer-readable medium having program instructions stored thereon to perform a method, which when executed within an electronic device, result in:

receiving, at a gaming system terminal, a plurality of data packets that includes an encrypted executable software program;

decrypting the encrypted executable software program to form a decrypted version of an executable software program;

authenticating the decrypted version of the executable software program using a predetermined criteria; and

enabling execution of the decrypted version of the executable software program when the decrypted version of the executable software program is determined to be authentic.